Amendments to the Claims:

Please enter the amendments reflected in the following listing of claims, which will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1 (original). A method of accessing a storage area network (SAN), comprising:

retrieving a first value from a first copy of a password table;

using the first value to retrieve a second value from the first copy of the password table;

encrypting the first value according to a first copy of an encryption key;

sending the encrypted first value to a node of the SAN;

decrypting the encrypted first value according to a second copy of the encryption key;

using the decrypted first value to retrieve a third value from a second copy of the password table;

encrypting the third value according to the second copy of the encryption key and sending the encrypted third value back to a switch of the SAN;

decrypting the third value according to the first copy of the encryption key and comparing the decrypted third value with the second value; and

allowing access to the SAN if the third value and the second value match.

2 (original). A method of claim 1, further comprising:

responsive to an event selected from a power on event and a software reset event, reading a serial identification corresponding to a host;

generating a code value based upon the serial number;

comparing the generated code value with a previously determined code value; and

denying access to the SAN if the generated code value and the previously determined code value differ.

3 (original). The method of claim 2, wherein the code value is further based on a time stamp and date stamp.

4 (original). The method of claim 1, wherein the SAN is a Fibre Channel compliant SAN.

5 (original). The method of claim 1, further comprising, periodically executing a key generation application that generates a unique password table and encryption key for each node attached to the SAN.

6 (previously presented). The method of claim 1, wherein retrieving the first value comprises randomly accessing an entry in the first copy of the password table and retrieving the first value from the randomly accessed entry.

7 (previously presented). The method of claim 6, wherein using the first value to retrieve a second value comprises hashing the first value to determine a second entry in the password table and retrieving the second value from the second entry.

8 (previously presented). The method of claim 1, wherein the password tables and encryption keys for each node are distributed over an encrypted link.

9-18 (canceled).

19 (original). A computer program product comprising a computer readable storage medium containing instructions for authorizing access to a storage area network, the instructions comprising:

a retriever enabled to retrieve a first value from a first copy of a password table;

means for using the retriever and the first value to retrieve a second value from the first copy of the password table;

an encryptor for encrypting the first value according to a first copy of an encryption key;

means for sending the encrypted first value to a node of the SAN;

a decryptor for decrypting the encrypted first value according to a second copy of the encryption key;

means for using the decrypted first value to retrieve a third value from a second copy of the password table;

means for encrypting the third value according to the second copy of the encryption key and sending the encrypted third value back to a switch of the SAN;

means for decrypting the third value according to the first copy of the encryption key and comparing the decrypted third value with the second value; and

means for allowing access to the SAN if the third value and the second value match.

20 (original). The computer program product of claim 19, further comprising:

a reader enabled to determine a serial identification corresponding to a host in response to an detecting an event selected from a power on event and a software reset event;

a code value generator enabled to generate a code value based upon the serial number;

a comparator enable to compare the generated code value with a previously determined code value; and

means for denying access to the SAN if the generated code value and the previously determined code value differ.

21 (original). The computer program product of claim 20, wherein the code value is further based on a time stamp and date stamp.

22 (original). The computer program product of claim 19, further comprising, a key generation application that generates a unique password table and encryption key for each node attached to the SAN.